

EXHIBIT 1

Not for Publication

**UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY**

THE CHILDREN’S PLACE, INC.,

Plaintiff,

v.

**GREAT AMERICAN INSURANCE
COMPANY,**

Defendant.

Civil Action No. 18-11963 (ES) (JSA)

OPINION

SALAS, DISTRICT JUDGE

Before the Court are cross-motions for summary judgment filed by plaintiff The Children’s Place, Inc. (“TCP”) (D.E. No. 68) and defendant Great American Insurance Company (“GAIC”) (D.E. No. 73), and a motion for leave to file a motion to strike and for sanctions filed by GAIC (D.E. No. 78). Having considered the parties’ submissions, the Court decides this matter without oral argument. *See* Fed. R. Civ. P. 78(b); L. Civ. R. 78.1(b). For the following reasons, TCP’s motion for summary judgment is DENIED, GAIC’s motion for summary judgment is GRANTED, and GAIC’s motion for leave is DENIED as moot.

I. BACKGROUND¹

A. Email-Fraud Scheme

TCP is a clothing company who, in June 2017, was the victim of a nearly \$1,000,000 email-fraud scheme perpetrated by an unidentified third party, hereinafter referred to as “the Thief.” (Joint SUMF ¶¶ 22, 26 & 94). The Thief hacked into the computer system—not of TCP—but of one of its vendors, Universal Apparel Co., Ltd. (“Universal”), and gained access to the email accounts of Universal employees. (*Id.* ¶ 26). Relying on information it obtained through this access, the Thief created virtually identical email domains to those of Universal employees. (*Id.* ¶¶ 26–27). What followed was a series of spoofed email exchanges between TCP and the Thief, who purported to be several different Universal employees. (*Id.* ¶¶ 29–90).

On June 13, 2017, the Thief, posing as a Universal employee, sent the first spoofed email to TCP, informing it that Universal’s bank was undergoing an audit and instructing it to send payments concerning invoices to SITI UMIROH, a purported sub-branch of Universal. (*Id.* ¶¶ 31, 39 & 43). The Thief sent this information on a letter (the “June 13 Letter”) containing Universal’s letterhead and a signature reflecting Universal’s Chief Financial Controller. (*Id.* ¶ 40). In response, TCP sent the Thief a [REDACTED] in order to obtain bank account information and payment instructions. (*Id.* ¶ 45). After receiving the [REDACTED], the Thief sent an email to Universal, making it appear to come from TCP, and requested that Universal [REDACTED]. (*Id.* ¶¶ 47–48).

¹ Unless noted otherwise, the following facts are not in dispute and are taken from the parties’ joint statement of undisputed material facts. (D.E. No. 71 (“Joint SUMF”)). In light of the Court’s analysis of the issues, the Court need not address the factual disputes arising out of TCP’s supplemental statement of undisputed facts. (*See* D.E. No. 72, TCP’s Supplemental Undisputed Facts; D.E. No. 74-3, GAIC’s Response to TCP’s Supplemental Statement). Those disputes relate to (i) the purpose of a discrete act committed by the perpetrator of a fraud scheme, and (ii) whether TCP continues to have a payment obligation to its vendor. (*Id.*).

The Thief, still posing as a Universal employee, continued to communicate with TCP employees over a period of six weeks. (*Id.* ¶ 22). In an email on June 30, 2017, the Thief sent a spreadsheet to multiple TCP employees, indicating current and upcoming invoices and directing payment for the specific amounts due. (*Id.* ¶ 67). After several back and forth emails in which the Thief demanded immediate payment, TCP issued a payment, on July 14, 2017, in the amount of \$498,753.58 to a fraudulent bank account operated by the Thief. (*Id.* ¶¶ 69–85). Three days later, and after another demand from the Thief, TCP issued a second payment in the amount of \$468,960.71. (*Id.* ¶¶ 90–91). The total of the two transfers was \$967,714.29. (*Id.* ¶ 94).

Before making the transfers, TCP did not call Universal to confirm the request to change its bank account information. (*Id.* ¶ 93). To date, TCP has been unable to recover the funds transferred to the Thief’s account and has not issued payments to Universal for the goods Universal provided to TCP. (*Id.* ¶¶ 97 & 110).

B. Insurance Coverage

TCP is insured by GAIC under a “Crime Protection Policy” (the “Policy”). (*Id.* ¶ 1). Relevant here, TCP purchased coverage for (i) Computer Fraud Loss, (ii) Forgery and Alteration Loss, and (iii) Fraudulently Induced Transfers. (*Id.* ¶¶ 3–4 & 11).

Under the Computer Fraud Loss provision, GAIC will

cover loss resulting directly from the use of any computer to impersonate you, or your authorized officer or employee, to gain direct access to your computer system, or to the computer system of your financial institution, and thereby fraudulently cause the transfer of money, securities or other property from your premises or banking premises to a person, entity, place or account outside of your control.

(*Id.* ¶ 5). Additionally, the Policy excludes from coverage under this provision any loss resulting from “[TCP’s] failure to comply with security procedures that [TCP] represented to [GAIC it]

would follow.” (*Id.* ¶ 6). The Policy defines “security procedures” as “a procedure established by agreement of the Insured and its customer or financial institution for the purpose of (i) verifying that a payment order is that of the Insured, or (ii) detecting error in transmission or the content of the payment order or communication.” (*Id.* ¶ 7). A security procedure may involve “the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices.” (*Id.*).

The Forgery and Alteration Loss provision covers “loss resulting directly from forgery or alteration of checks, drafts, promissory notes, or similar written promises, orders, or directions to pay a sum certain in money that are . . . made or drawn by or drawn upon [TCP].” (*Id.* ¶ 8). The Policy defines “forgery” as “the signing of the name of another person or organization with intent to deceive; it does not mean a signature which consists in whole or in part of one’s own name signed with or without authority, in any capacity, for any purpose.” (*Id.* ¶ 9). Further, the provision contains a condition related to “Facsimile Signature,” which states “[GAIC] will treat a reproduction of a handwritten signature the same as handwritten signature. An electronic or digital signature is not treated as a reproduction of a handwritten signature.” (*Id.* ¶ 10).

Finally, the Fraudulently Induced Transfers provision covers “losses resulting directly from fraudulently induced transfers”—so long as TCP verifies any change in bank account information by calling its vendor at a predetermined number. (*Id.* ¶ 15).

Following the fraudulent scheme described above, TCP submitted its losses to GAIC for coverage under the Policy. (*Id.* ¶ 123). On May 25, 2018, GAIC denied coverage for TCP’s claimed losses. (*Id.* ¶ 124).

C. Procedural History

On July 23, 2018, TCP filed a complaint against GAIC for declaratory relief and breach of contract; for both counts, TCP claimed it was entitled to coverage under the Policy’s provisions for Computer Fraud Loss, Forgery and Alteration Loss, and Fraudulently Induced Transfers. (D.E. No. 1 ¶¶ 25–30 & 58–66). GAIC moved to dismiss the complaint (D.E. No. 4), and the Court granted in part and denied in part the motion, holding that TCP stated a claim under the Computer Fraud Loss provision but failed to state claims under the Forgery and Alteration Loss and Fraudulently Induced Transfers provisions (D.E. No. 16 (“Apr. 25 Op.”) at 4). As to the Forgery and Alteration Loss provision, the Court held that the [REDACTED] and the June 13 Letter did not “promise, order, or direct the payment of a ‘sum certain.’” (*Id.* at 8). And as to the Fraudulently Induced Transfers provision, the Court explained that TCP failed to satisfy a condition precedent to coverage—that is, to call Universal at a predetermined number to verify routing and account numbers before making a payment. (*Id.* at 9–10). The Court dismissed those claims without prejudice. (*Id.* at 10–11). TCP filed an amended complaint, reviving its claim under the Forgery and Alteration Loss provision. (D.E. No. 21). TCP did not amend its complaint to revive its claim under the Fraudulently Induced Transfers provision. TCP and GAIC have cross-moved for summary judgment.

II. LEGAL STANDARD

Summary judgment is appropriate “if the movant shows there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law.” Fed. R. Civ. P. 56(a). A genuine issue of material fact exists when—in viewing the evidence and all reasonable inferences drawn from it in the light most favorable to the nonmovant—a reasonable jury could return a verdict for the nonmoving party. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248

(1986). The movant bears the burden of establishing that no “genuine issue” of facts exists. *Aman v. Cort Furniture Rental Cop.*, 85 F.3d 1074, 1080 (3d Cir. 1996).

III. DISCUSSION

The central two issues in this case—whether the losses TCP suffered from the above-described email-fraud scheme are covered under the Computer Fraud Loss provision and/or the Forgery and Alteration Loss provision—present issues of law. Meanwhile, whether TCP is entitled to certain fees that it paid to a forensic investigator (described below) presents both factual and legal questions. The Court concludes that TCP’s losses are not covered under either provision, that the investigator’s fees are not covered as losses under either provision, and that other asserted theories for recovery of the investigator’s fees are not properly before the Court.

A. Computer Fraud Loss Provision

The Court must determine whether the Thief’s email-fraud scheme imposed a loss on TCP that is covered under the Computer Fraud Loss provision. Neither party disputes the facts relevant to this issue, and the Court outlined those facts above. Instead, the parties dispute whether the scheme is one that falls within the Computer Fraud Loss provision.

As noted above, under the Computer Fraud Loss provision, GAIC will

cover loss resulting directly from the use of any computer to impersonate you, or your authorized officer or employee, to gain direct access to your computer system, or to the computer system of your financial institution, and thereby fraudulently cause the transfer of money, securities or other property from your premises or banking premises to a person, entity, place or account outside of your control.

(Joint SUMF ¶ 5). TCP agrees that, to establish coverage under this provision, it must show (i) that it suffered a direct loss from the use of a computer; (ii) that a computer was used to gain direct access to its computer system; and (iii) that said access caused money to be fraudulently transferred

to an account outside of its control. (D.E. No. 69 (“Pl. Mov. Br.”) at 6). Because the second element is dispositive, and because TCP does not satisfy it, the Court will focus on the meaning of “direct access.”

TCP argues that the Thief gained direct access to TCP’s computer system by sending the spoofed emails—because those emails “entered and communicated with TCP’s computer system.” (*Id.* at 9). In support, TCP lays out several definitions of “direct” and “access.” (*Id.* at 10–11). The term “direct,” TCP says, means to be “marked by absence of an intervening agency, instrumentality, or influence” or to be “free from extraneous influence; immediate.” (*Id.* at 10 (first quoting the definition of “direct” in the online version of Merriam-Webster, and then quoting the same in Black’s Law Dictionary)). And the term “access,” TCP further claims, means the “ability to enter, approach, or pass to and from a place or to approach or communicate with a person or thing” or a “right, opportunity, or ability to enter, approach, pass to and from, or communicate with.” (*Id.* (first quoting the definition of “access” in the online version of Merriam-Webster, and then quoting the same in Black’s Law Dictionary)). It follows, according to TCP, that the “direct access” element is satisfied where, as here, a person had the “immediate ability – without any outside influence – to communicate with and enter TCP’s computer system and, in fact, did communicate with and enter TCP’s computer system through the exchange of emails.” (*Id.* at 10–11).

GAIC responds that TCP’s argument is without merit. (D.E. No. 74-1 (“Def. Mov. & Opp. Br.”) at 14–15). TCP’s argument, GAIC says, is basically that by merely sending an email, a person gains direct access to the recipient’s computer system. (*Id.* at 14). That interpretation is implausible, GAIC goes on, because it “would mean that anybody in the world can gain ‘direct

access’ to this Court’s computers by simply sending emails to addresses registered with the domain ‘njd.uscourts.gov.’” (*Id.* at 14).

If an unknown person called the Court and claimed to have “gain[ed] direct access” to a federal judge’s computer, however, it is highly unlikely that the Court would interpret the statement to mean the caller had sent an ordinary email. Instead, the Court would likely understand the statement as a serious threat involving the integrity of a federal judge’s secure computer system.

(D.E. No. 74-2, Defendant’s Reply at 10–11). “The use of the phrase ‘direct access,’” GAIC concludes, “to describe sending an email to a publicly-accessible email account simply does not make sense.” (*Id.* at 10).

The Court agrees with GAIC. Under New Jersey law, a court must give “the words of an insurance policy . . . their ordinary meaning.” *Longobardi v. Chubb Ins. Co. of New Jersey*, 582 A.2d 1257, 1260 (N.J. 1990). New Jersey courts have repeatedly stressed that “[l]iteralism must give way to context.” *E.g., Phoenix Pinelands Corp. v. Davidoff*, No. A-2823-16, 2021 WL 1679682, at *57 (N.J. Super. App. Div. Apr. 29, 2021) (citations omitted). While dictionary definitions are relevant to this task, they are not dispositive, and a court must consider the policy’s terms “in the context that they appear” and “be wary of interpretations that render other policy terms meaningless.” *Formosa Plastics Corp., U.S.A. v. ACE Am. Ins. Co.*, No. 06-5055, 2010 WL 4687835, at *6 (D.N.J. Nov. 9, 2010) (citing *Hardy ex rel. Dowdell v. Abdul-Matin*, 965 A.2d 1165, 1170 (N.J. 2009)). Thus, for example, in *Morton International Inc. v. General Accident Insurance Company of America*, 629 A.2d 831 (N.J. 1993), the New Jersey Supreme Court declined to give the term “damages” its literal meaning—that being, all types of damages—because “the term ‘damages’ is not ambiguous,” in that its plain meaning, “as used in the insurance context[,] refers to legal damages and does not include equitable monetary relief.” *Id.* at 844–45.

Likewise, although the combination of “direct” and “access” may literally include the “immediate ability” to “enter and communicate,” that is not what it means in the context of an insurance policy that governs direct access to an inanimate object (a computer system) with which one would not ordinarily say he or she “communicates.” Indeed, as GAIC points out, every term in the Computer Fraud Loss provision “must be considered in the context . . . [of] describing the nature of an interaction with a ‘computer system.’” (Def. Mov. & Opp. Br. at 15). TCP’s literalist interpretation ignores that context, and by asking the Court to adopt it, TCP asks the Court to alter the plain and ordinary meaning of the phrase “direct access” by “applying a generic definition of the word ‘access’ that has nothing to do with computers.” (*Id.* at 16).

Moreover, interpreting the Computer Fraud Loss provision otherwise would, effectively, convert it into a general fraud provision because “few—if any—fraudulent schemes would not involve some form of computer-facilitated communication.” *See Apache Corp. v. Great Am. Ins. Co.*, 662 F. App’x 252, 258 (5th Cir. 2016). Thus, while it is not dispositive, the fact that the Policy has a separate provision that covers general fraud—that is, the Fraudulently Induced Transfers provision—suggests that the Computer Fraud Loss provision was not intended by the parties to cover general fraud. Indeed, in the digital age, such an interpretation could plausibly render the Fraudulently Induced Transfers provision meaningless, a result the Court must avoid. *See Homesite Ins. Co. v. Hindman*, 992 A.2d 804, 807 (N.J. Super. App. Div. 2010) (“We will not read one policy provision in isolation when doing so would render another provision meaningless.”).

The above interpretation is supported by courts in other jurisdictions interpreting the same or materially similar provisions. In *Sanderina, LLC v. Great American Insurance Company*, No. 18-0772, 2019 WL 4307854 (D. Nev. Sept. 11, 2019), a district court, interpreting the same

provision at issue here, held that the act of sending an email to the insured's computer does not constitute direct access to the insured's computer system. *Id.* at *3. The court reasoned that the "direct access" element in the disputed policy was akin to policies limiting coverage to "entry into," which suppose a sort of actionable trespass into the insured's computer system. *Id.* (citing *Taylor & Lieberman v. Fed. Ins. Co.*, 681 F. App'x 627, 629 (9th Cir. 2017)). In *Taylor*, 681 F. App'x 627, the Ninth Circuit explained that "the 'mere sending' of emails does not amount to actionable trespass to," and thus does not constitute entry into, "a computer system in the absence of 'some actual or threatened interference with the computers' functioning.'" *Id.* at 629 (quoting *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 1353, 71 P.3d 296, 304 (2003)). In the context of direct access to a computer system, the Court finds these views persuasive.

TCP's other arguments to the contrary are not persuasive. First, TCP argues that its interpretation should prevail because, under New Jersey law, ambiguity in an insurance contract should be construed in favor of the insured. (Pl. Mov. Br. at 5 (citing *Nav-Its, Inc. v. Selective Ins. Co. of Am.*, 869 A.2d 929, 933 (N.J. 2005))). However, TCP admits that this interpretive rule does not apply where the insurance policy is unambiguous. (*Id.*). Indeed, absent such ambiguity, "a court should not engage in a strained construction to support the imposition of liability." *Longobardi*, 582 A.2d at 1260. As discussed above, the Computer Fraud Loss provision unambiguously does not favor TCP's interpretation.

Second, TCP argues that GAIC has "repeatedly – and improperly – attempted to impose a heightened standard" by requiring "that the Thief hack, log into, or install malware on TCP's computer system." (Pl. Mov. Br. at 11). However, GAIC's interpretation properly considers the provision both in its entirety and in light of its context, as discussed above.

Third, TCP argues that its interpretation should prevail because a forensic investigator, Mandiant,² concluded that the Thief “accessed” and “entered” TCP’s computer system by sending the spoofed emails. (Pl. Mov. Br. at 11 (citing Joint SUMF ¶¶ 119–21)). TCP hired Mandiant to perform a “thorough and comprehensive forensic examination of TCP’s computer systems and email accounts.” (Joint SUMF ¶ 104). To that end, Mandiant prepared a report dated September 25, 2017, and a revised report dated May 23, 2019. (*Id.* ¶¶ 105 & 115).

However, Mandiant’s opinion is not relevant to the legal question addressed above. TCP itself concedes, “the Court does not require expert testimony to interpret the words ‘direct access’ under the Policy.” (D.E. No. 70 (“Pl. Opp. & Reply Br.”) at 11). Indeed, the Court does not. Be it a contract or a statute, “[e]xpert witnesses simply may not render opinions on matters which involve a question of the law.” *Boddy v. Cigna Prop. & Cas. Companies*, 760 A.2d 823, 828 (N.J. Super. App. Div. 2000) (quoting *Healy v. Fairleigh Dickinson Univ.*, 671 A.2d 182, 184 (N.J. Super. App. Div. 1996)); *see also Kamienski v. State, Dep’t of Treasury*, 169 A.3d 493, 505 (N.J. Super. App. Div. 2017) (“An expert’s opinion on a question of law is neither appropriate nor probative.”). Even still, Mandiant’s opinion is not particularly helpful. As GAIC points out, Mandiant offered the opinion in the revised report, which Mandiant did not intend to change any of its previous conclusions. (Def. Mov. & Opp. Br. at 16 & 18). One of those previous conclusions was that there was no “evidence that a third party ‘hacked, logged into, or otherwise gained unauthorized access to any of TCP’s computer systems or email accounts.’” (*Id.* at 13). And, as GAIC further points out, Mandiant “testified that the emails at issue ‘did not result in any third party gaining access to an internal computer system belonging to TCP.’” (*Id.* at 16 (quoting Joint

² Mandiant is the organization that the forensic investigator works for, not the forensic investigator’s name. The Court refers to the forensic investigator as Mandiant because TCP has maintained, and GAIC does not dispute, that the identity of the forensic investigator should remain confidential. (D.E. No. 75, TCP’s Supplement to Motion to Seal ¶ 7).

SUMF ¶ 112)). Consequently, Mandiant's opinion does not change the fact that the Thief did not gain direct access to TCP's computer system by simply sending a series of spoofed emails.

Accordingly, GAIC is entitled to summary judgment on TCP's claim that it is entitled to coverage under the Computer Fraud Loss provision.

B. Forgery and Alteration Loss Provision

The Court must also determine whether the Thief's email-fraud scheme imposed a loss on TCP that is covered under the Forgery and Alternation Loss provision. Neither party disputes the facts relevant to this claim. The issue is thus whether the email-fraud scheme, described above, produced a covered forgery or alteration. As relevant here, coverage under the Forgery and Alteration Loss provision requires that there (i) be a loss; (ii) "resulting directly from"; (iii) "forgery or alteration"; (iv) "of checks, drafts, promissory notes, or similar written promises, orders, or directions to pay a sum certain in money that are"; (v) "made or drawn upon" TCP. (Joint SUMF ¶ 8).

TCP argues that the losses it suffered from the email-fraud scheme are covered under the Forgery and Alteration Loss provision because the Thief "used multiple forged documents to fraudulently induce payment from TCP." (Pl.'s Mov. Br. at 18). The documents TCP specifically refers to are (i) the [REDACTED], (ii) the June 13 Letter, (iii) spoofed email communications, and (iv) a spreadsheet stating outstanding Universal invoices. (*Id.*).

However, not one of those documents independently satisfies each element of the Forgery and Alternation Loss provision.

First, the Court previously held, when dismissing TCP's original complaint, that the [REDACTED] and the June 13 Letter do not reference "a sum certain in money," as required

under this provision. (Apr. 25 Op. at 9). Though TCP filed an amended complaint, TCP has not provided any evidence to show otherwise.

Second, while the spoofed email communications demand payments, and while some of the emails contain signatures, not one of those emails was forged or altered. The Policy defines “forgery” as “the signing of the name of another person or organization with intent to deceive; it does not mean a signature which consists in whole or in part of one’s own name signed with or without authority, in any capacity, for any purpose.” (Joint SUMF ¶ 9). Further, the Policy contains a condition related to “Facsimile Signature,” which provides that “[GAIC] will treat a reproduction of a handwritten signature the same as handwritten signature. An electronic or digital signature is not treated as a reproduction of a handwritten signature.” (*Id.* ¶ 10). The spoofed emails are not forgeries because, as GAIC correctly points out, the policy explicitly “does not treat an electronic or digital signature as a reproduction of a handwritten signature . . . [and so] it cannot be a ‘forgery.’” (Def. Mov. & Opp. Br. at 35). Notably, TCP concedes that it “has not taken the position that an email constituted a forgery.” (Pl. Opp. & Reply Br. at 22). And the spoofed emails clearly are not alterations. Although the policy does not define the term “alteration,” Black’s Law Dictionary defines it as “an act done to an instrument, after its execution, whereby its meaning or language is changed; esp., the changing of a term in a negotiable instrument without the consent of all parties to it.” Alteration, Black’s Law Dictionary (11th ed. 2019). Because the content of the spoofed emails did not change after their original execution—indeed, they were originally executed by the Thief—the emails were not altered.

Third, while TCP plausibly argues that the spreadsheet is akin to a direction to pay a sum certain in money (Pl. Mov. Br. 19–20), the spreadsheet is neither a forgery nor an alternation. The spreadsheet does not, as GAIC points out, “contain any marks that could even arguably be

described as a signature, much less a signature that falls within the policy’s definition of ‘forgery.’” (Def. Mov. & Opp. Br. at 36). Nor does the spreadsheet constitute an alteration. As with the spoofed emails, there is no indication that anything was done to the spreadsheet after it was originally executed, and it appears to have been originally executed by the Thief.

TCP appears to admit as much—that is, that it cannot point to a single document, email, or communication that can alone satisfy each element of the Forgery and Alteration Loss provision. To cure that defect, TCP argues that the documents and emails, when “[v]iewed together,” satisfy the provision. (Pl. Mov. Br. at 19). Said another way, TCP would have the Court read the provision as allowing it to offer various documents—some of which satisfy a couple elements and the rest of which satisfy the remaining elements. But TCP has not pointed to any language in the policy suggesting that such an approach is appropriate. And that approach fails to account for the preposition “of” in the Forgery and Alteration Loss provision. Indeed, while TCP’s losses may have resulted from a forgery (e.g., the June 13 Letter), it did not result from a “forgery or alteration of” checks, drafts, promissory notes, or similar written promises, orders, or directions to pay a sum certain in money. (Joint SUMF ¶ 8 (emphasis added)).

To be sure, some “[c]ourts have occasionally bundled documents in situations in which [a] bank demanded all involved documentation to extend credit or honor a draft.” *Travelers Cas. & Sur. Co. of Am. v. Baptist Health Sys.*, 313 F.3d 295, 299 (5th Cir. 2002) (citing *Omnisource Corp. v. CNA/Transcon. Ins. Co.*, 949 F. Supp. 681, 686 (N.D. Ind. 1996); *Cnty. State Bank of Galva v. Hartford Ins. Co.*, 187 Ill. App. 3d 110, 114, 542 N.E.2d 1317, 1320 (1989)). And, though not precisely for that proposition, TCP cites at least one of those cases (*Omnisource*) in its opposition and reply brief. (Pl. Opp. & Reply Br. at 24). However, the Court agrees with the Fifth Circuit

that those cases do not extend where, as here, not all of the involved documents were required to induce payment from a bank. *Travelers Cas. & Sur. Co. of Am.*, 313 F.3d at 299.

Accordingly, GAIC is entitled to summary judgment on TCP's claim that it is entitled to coverage under the Forgery and Alteration Loss provision.

C. Costs Associated with Mandiant

Finally, the Court must determine whether TCP may recover fees it paid to a forensic investigator, Mandiant, in the amount of \$42,200.00, for 105.5 billed hours. (Pl. Mov. Br. at 21). As noted above, TCP hired Mandiant to perform a "thorough and comprehensive forensic examination of TCP's computer systems and email accounts." (Joint SUMF ¶ 104). TCP claims it is entitled to recover the fees paid to Mandiant as (i) a loss covered under the Policy, (ii) a mitigation expense to avoid future losses, and/or (iii) a claims expense. (Pl. Mov. Br. at 21–24). GAIC opposes TCP recovering Mandiant's fees and, in response, moves for leave to file a motion to strike and for discovery sanctions. (D.E. No. 78).

(i) Loss

TCP argues that Mandiant's fees constitute a direct loss under the Computer Fraud Loss and Forgery and Alteration Loss provisions because TCP incurred them as a result of the email-fraud scheme. (Pl. Mov. Br. at 22). But as set forth above, the email-fraud scheme is not covered under either of those provisions. Consequently, nor are Mandiant's fees.

(ii) Mitigation Expense and Claims Expense

TCP claims that it may recover Mandiant's fees as a "mitigation expense," which it claims is recoverable under New Jersey law. (Pl. Mov. Br. at 23). In support, TCP argues that it retained Mandiant as part of its mitigation efforts—"for the purpose of ensuring the threat posed by the Thief was neutralized." (*Id.*). TCP separately argues that it may recover Mandiant's fees "under

the Policy's coverage for claims expense." (*Id.* at 24). The claims expense provision provides:

The Company shall reimburse the Insured for 50% of the claims expense of the Insured on any paid claim, up to the limit of \$100,000.

Claims expense means reasonable expenses incurred by the Insured in establishing the existence and amount of any direct loss covered in excess of the Deductible amount of this Policy, as stated in the Declarations. The reasonableness of such expenses shall be determined by the Company and shall not include internal corporate obligations of the Insured, such as employee wages or internal costs.

(*Id.* (quoting D.E. No. 71-1, Ex. A, Policy, Endorsement No.16, Expense Coverage)). TCP argues that, because Mandiant's services "were incurred, in part, to establish the existence of a direct loss under the Policy," it is entitled to 50% of Mandiant's fees. (*Id.*).

However, TCP's amended complaint does not assert independent claims for Mandiant's fees as a mitigation expense or a claims expense. Instead, TCP sought Mandiant's fees as a portion of damages caused by the email-fraud scheme and covered under the Computer Fraud Loss and Forgery and Alteration Loss provisions. As briefed by TCP, those claims have different elements than claims for coverage as a mitigation expense or a claims expense. For example, TCP concedes that coverage as a mitigation expense is "a separate and independent basis for coverage" that exists pursuant to New Jersey law, not the Crime Protection Policy. (Pl. Mov. Br. at 23). However, the amended complaint does not assert claims separate and independent of the Crime Protection Policy. Moreover, while the provision for claims expenses falls within the Crime Protection Policy, the amended complaint does not hint at the possibility that TCP would seek Mandiant's fees as a claims expense. Indeed, the amended complaint does not allege, much less suggest, that Mandiant's fees were reasonable or that GAIC exceeded its discretion in determining that Mandiant's fees were unreasonable. The text of the claims expense provision appears to require at least those two elements for coverage.

Because TCP may not amend its complaint when seeking summary judgment, the Court will not consider TCP's unpled claims. *See Berrada v. Cohen*, 792 F. App'x 158, 162 n.3 (3d Cir. 2019) ("Berrada also argues that he had an 'enforceable verbal agreement' or an implied-in-fact contract. Berrada's complaint asserted a breach of 'express terms' of the July 16, 2014 written offer, and so we will not consider an unpled implied-in-fact contract claim." (internal citations omitted)); *Bell v. City of Philadelphia*, 275 F. App'x 157, 160 (3d Cir. 2008) (finding First Amendment claim did not include "right to petition" theory and, therefore, could not be raised in opposition to summary judgment); *id.* ("At the summary judgment stage, the proper procedure for plaintiffs to assert a new claim is to amend the complaint in accordance with Fed.R.Civ.P. 15(a)." (quoting *Gilmour v. Gates, McDonald & Co.*, 382 F.3d 1312, 1315 (11th Cir. 2004))); *Carr v. Gillis Associated Indus., Inc.*, 227 F. App'x 172, 176 (3d Cir. 2007) ("District Courts have broad discretion to disallow the addition of new theories of liability at the eleventh hour."); *Krouse v. Am. Sterilizer Co.*, 126 F.3d 494, 499 n.1 (3d Cir. 1997) ("Although a complaint's allegations are to be construed favorably to the pleader, we will not read causes of action into a complaint when they are not present. The ADA is one statutory scheme, but it provides more than one cause of action. Where, as here, a plaintiff asserts a cause of action for retaliation under 42 U.S.C. § 12203(a), we will not find an implicit cause of action for failure to accommodate under 42 U.S.C. § 12112(a)." (internal citation omitted)); *Oh v. Collecto, Inc.*, No. 20-01937, 2021 WL 3732881, at *4 (D.N.J. Aug. 23, 2021) (holding that plaintiff could not raise new theory of standing at summary judgment).

Accordingly, GAIC is entitled to summary judgment on the issue regarding Mandiant's fees. Thus, GAIC's separately filed motion for leave to file a motion to strike and for discovery sanctions (D.E. No. 78) is denied as moot.

IV. CONCLUSION

For the foregoing reasons, TCP's motion for summary judgment (D.E. No. 68) is DENIED, and GAIC's motion for summary judgment (D.E. No. 73) is GRANTED. Judgment is entered in GAIC's favor. GAIC's motion for leave to file a motion to strike and for discovery sanctions (D.E. No. 78) is DENIED as moot. An appropriate Order will follow.

Dated: September 28, 2021

/s/Esther Salas
Esther Salas, U.S.D.J.